Livre blanc sur la sécurité et la confidentialité de la plateforme cloud européenne destinée aux solutions logicielles médicales

Responsable éditorial	Digital Services Operations Fresenius Medical Care Deutschland GmbH Else-Kröner-Str. 1 D - 61352 Bad Homburg v.d.H. Téléphone : +49 (0) 6172-609-7000 +49 (0) 6172-609-7000 Courrier : digital.services.EMEA@freseniusmedicalcare.com

Table des matières

1. Introduction

Ce document décrit les aspects de sécurité liés à l'exploitation et au déploiement de la plateforme cloud de Fresenius Medical Care EU. Cette plateforme constitue la base opérationnelle des solutions métiers basées sur le cloud et permet de fournir des services et des solutions informatiques de base et avancés aux cliniques et aux patients au sein de l'UE.

L'exploitation sécurisée, stable et conforme aux exigences légales constitue la base pour ces nouveaux types de services cloud. Un fonctionnement fiable est essentiel pour Fresenius Medical Care et ses clients, nécessitant une haute disponibilité sur l'ensemble de la zone géographique concernée. Nos services cloud sont conçus pour offrir une sécurité supérieure à celle de nombreuses solutions traditionnelles sur site. La sécurité est donc essentielle pour protéger nos opérations.La sécurisation de nos services cloud ainsi que de notre infrastructure informatique constitue une priorité stratégique pour notre activité.

1.1 Applications

Les applications et solutions sont développées sur une plateforme sécurisée bénéficiant de services fortement protégés. Par conséquent, les sujets spécifiques aux applications sont exclus et ne font pas partie de ce document.

Les unités de développement EMEA appliquent une procédure opératoire standard interne (POS) intitulée « Politique de codage sécurisé », basée sur une approche fondée sur les risques et intégrant les méthodes et contrôles de la norme ISO 27001.

La sécurité est intégrée dès la conception et respecte les normes industrielles ainsi que les meilleures pratiques. De plus, la cybersécurité et l'évaluation des risques font partie intégrante du processus de développement et du concept opérationnel.

2. Protection des données personnelles et confidentialité

Le service de plateforme offre un environnement sécurisé pour l'exécution des applications. Pour toute information relative à la sécurité applicative, veuillez consulter la documentation dédiée. Le système de production est opéré exclusivement depuis l'UE. Tout accès aux données de nos clients fait l'objet d'une traçabilité rigoureuse et s'effectue uniquement de manière transactionnelle. L'hébergement des données ainsi que les équipes opérationnelles sont localisés au sein de l'UE.

Fresenius Medical Care met en œuvre des dispositifs stricts afin de garantir la confidentialité des données de ses clients et de limiter les demandes excessives, dans le respect de ses obligations légales. Le règlement général sur la protection des données (RGPD) est appliqué selon le principe de « privacy by design », avec l'implication du Délégué à la Protection des Données (DPO) et du service juridique. La protection de la vie privée et de la sécurité des données que vous stockez sur le cloud de Fresenius Medical Care constitue une priorité, tout en assurant le respect des demandes légales encadrées par la réglementation en vigueur.

3. Sécurité des personnes

3.1 Formations de sensibilisation

Les collaborateurs de Fresenius Medical Care sont formés aux politiques internes de l'entreprise et aux bonnes pratiques en matière de sécurité. Cela inclut une formation annuelle obligatoire à la sécurité ainsi que des actions régulières de sensibilisation aux risques et aux pratiques de cybersécurité. Tous les nouveaux collaborateurs de Fresenius Medical Care s'engagent à respecter les politiques de sécurité de l'information en vigueur et suivent une formation à la cybersécurité lors de leur intégration. Par ailleurs, l'ensemble des employés doit suivre et valider une formation dédiée à la protection des données personnelles, couvrant les bonnes pratiques en matière de confidentialité ainsi que les exigences réglementaires, notamment celles du Règlement Général sur la Protection des Données (RGPD).

3.2 Vérification des antécédents

Le processus de recrutement chez Fresenius Medical Care comprend des vérifications de références externes. Celles-ci peuvent inclure la validation des diplômes et des expériences professionnelles antérieures.Lorsque la législation locale ou les réglementations en vigueur le permettent, des vérifications complémentaires (judiciaires, financières, administratives ou liées au droit de séjour) peuvent être effectuées, en fonction de la juridiction concernée et du poste visé.

3.3 Formation des employés

Fresenius Medical Care assure une communication régulière sur les menaces émergentes et informe fréquemment ses collaborateurs des campagnes de phishing en cours.
Les employés sont invités à signaler sans délai tout incident de sécurité suspecté auprès des départements Sécurité de l'Information ou Informatique.

4. Sécurité opérationnelle

4.1 Sécurité des données

La protection des données clients est une priorité absolue pour Fresenius Medical Care. Pour la garantir, les serveurs sont sécurisés à l'aide de mécanismes de contrôle multi-couches et font régulièrement l'objet d'analyses de vulnérabilités. Tous les services intègrent des sauvegardes chiffrées, et les serveurs utilisent le protocole TLS (Transport Layer Security) à jour pour protéger les données transmises via Internet et les réseaux publics.

4.2 Contrôle des accès

Afin de garantir la confidentialité et la sécurité des données, celles des clients sont isolées logiquement, même lorsqu'elles sont hébergées sur le même serveur physique. Seul un nombre restreint de collaborateurs administratifs dispose d'un accès aux données des clients. Les droits d'accès sont attribués en fonction des rôles et responsabilités selon les principes du moindre privilège et du besoin d'en connaître. Par défaut, les collaborateurs disposent uniquement des autorisations minimales nécessaires à l'exercice de leurs fonctions.

4.3 Politique interne de gestion des identifiants

La politique de gestion des identifiants de Fresenius Medical Care encadre la création, la protection et la fréquence de rotation des identifiants. La complexité des mots de passe est conforme aux standards du secteur (longueur minimale, complexité élevée, politique de verrouillage, etc. dans le cadre de notre infrastructure Active Directory). Les identifiants sont transmis via des connexions sécurisées (HTTPS). Une solution de gestion des accès à privilèges (PAM) est utilisée pour contrôler, auditer et faire tourner les identifiants de manière sécurisée.

4.4 Gestion des secrets

Fresenius Medical Care applique les meilleures pratiques en matière de gestion des secrets. L'organisation s'appuie sur des outils reconnus pour leur sécurité et leur capacité à évoluer, en complément d'une politique rigoureuse de conservation et de rotation des mots de passe.

4.5 Chiffrement des données

Les clients bénéficient de connexions chiffrées de bout en bout via TLS, intégrées nativement à la plateforme. Les données en transit (via SSL, VPN, HTTPS) ainsi que les données au repos sont systématiquement chiffrées selon les méthodes les plus récentes et robustes.

4.6 Protection des terminaux

Les attaques par logiciels malveillants peuvent entraîner des compromissions de comptes, le vol de données ou des accès non autorisés au réseau. Fresenius Medical Care traite ces menaces avec la plus grande rigueur, en appliquant des stratégies de prévention, de détection et de remédiation. Les serveurs et postes de travail des collaborateurs sont protégés par des logiciels antivirus et suivent les meilleures pratiques du secteur.

4.7 Gestion des vulnérabilités

Le processus de gestion des vulnérabilités permet l'identification proactive des menaces à l'aide d'outils commerciaux et de méthodes internes. Il comprend des tests d'intrusion automatisés et manuels, des procédures d'assurance qualité, des revues de sécurité logicielle et des audits externes réguliers.

4.8 Tests d'intrusion

Fresenius Medical Care réalise régulièrement des tests d'intrusion, à la fois via ses équipes internes et des prestataires externes spécialisés. Grâce à des outils avancés de test de pénétration, l'organisation identifie les vulnérabilités potentielles et les vecteurs d'attaque, afin de mieux évaluer les risques et renforcer sa posture de cybersécurité.

4.9 Supervision et surveillance

La supervision se concentre sur l'analyse des flux internes, des activités des utilisateurs, ainsi que des informations issues de la veille sur les vulnérabilités externes. Des systèmes de détection des anomalies sont déployés sur l'ensemble du réseau global pour repérer les comportements suspects, les schémas de trafic inhabituels ou les connexions potentiellement malveillantes.

5. Sécurité physique

5.1 Sécurité des locaux

La sécurité physique des bureaux et installations de Fresenius Medical Care est définie et mise en œuvre conformément aux normes de sécurité internes de l'entreprise, afin de protéger les infrastructures contre les catastrophes naturelles, les accidents et les menaces malveillantes. Des périmètres de sécurité clairement définis et des procédures opérationnelles strictes garantissent la protection des zones hébergeant des informations sensibles ou critiques au sein des centres de traitement de l'information. L'accès aux locaux est rigoureusement contrôlé par des systèmes de badges physiques et de cartes d'accès, empêchant toute intrusion non autorisée. Une surveillance continue est assurée par des agents de sécurité ainsi que par des systèmes de vidéosurveillance.

5.2 Sécurité des centres de données

Les centres de données de Fresenius Medical Care sont répartis géographiquement et bénéficient de multiples dispositifs de sécurité physique. Les infrastructures respectent les normes de référence du

secteur en matière de sécurité physique et de contrôle environnemental. Fresenius Medical Care s'appuie sur Microsoft Azure pour l'hébergement de ses systèmes de production, en conformité avec les bonnes pratiques standardisées du secteur.

6. Continuité d'activité

6.1 Plan de continuité d'activité

Fresenius Medical Care dispose de plans formels de continuité d'activité et de reprise après sinistre, régulièrement révisés et mis à jour. L'entreprise a développé une stratégie robuste de continuité permettant une réponse rapide et une résilience durable face à divers types de perturbations, notamment les catastrophes naturelles et les défaillances systèmes.

6.2 Reprise après sinistre

Fresenius Medical Care met en œuvre un programme de reprise après sinistre déployé à l'échelle de l'organisation. Afin de prévenir toute perte de données, une réplication continue et des sauvegardes sont effectuées au sein de chaque centre de données. L'entreprise dispose d'un site de reprise qui garantit une continuité de service optimale et une perte de données minimale en cas de catastrophe naturelle ou de défaillance système.

6.3 Plan de réponse aux incidents

Fresenius Medical Care dispose d'un plan formalisé de réponse aux incidents (PRI) ainsi que d'une politique associée. Cette politique définit les processus d'identification, de classification, de signalement, de traitement et d'atténuation des incidents de sécurité, couvrant également les phases d'évaluation post-incident. Le département de sécurité des systèmes d'information de Fresenius Medical Care enquête rapidement sur toute anomalie ou suspicion d'incident de sécurité à l'échelle de l'entreprise.

6.4 Gestion des fournisseurs

Le département de sécurité des systèmes d'information de Fresenius Medical Care évalue les fournisseurs potentiels via un processus d'évaluation des risques et assure un suivi continu pour garantir le respect des normes de sécurité de l'entreprise.

7. Conformité réglementaire

Nos clients sont soumis à des exigences réglementaires variées. Ils évoluent principalement dans des environnements réglementés liés aux dispositifs médicaux et aux prestations de soins. Fresenius Medical Care s'assure d'obtenir les certifications nécessaires et respecte les exigences réglementaires applicables afin de garantir une exploitation sans faille des services proposés par nos solutions.
Les opérations cloud de base reposent sur les référentiels ISO 27001, ISO 27002, ISO 27017, ISO 27018 ainsi que la certification HDS (Hébergeur de Données de Santé) en France, qui constituent le socle de l'exploitation des infrastructures et des fournisseurs de services cloud sous-jacents. Fresenius Medical Care respecte la législation en vigueur dans l'Union Européenne.

7.1 Attestation de transfert de données pour la certification HDS

Fresenius Medical Care ne transfère pas de données de santé à caractère personnel en dehors de l'Espace économique européen (EEE).